Załącznik nr 26/2009 do Zarządzenia
Burmistrza Miasta i Gminy Ostrzeszów z dnia 31.03.2009

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA SYSTEMU OCHRONY DANYCH OSOBOWYCH

w

Urzędzie Miasta i Gminy w Ostrzeszowie

Ostrzeszów, 2009 r.

§1.

Instrukcja przeznaczona jest dla osób zatrudnionych przy przetwarzaniu danych osobowych

§2.

Instrukcja określa tryb postępowania w przypadku, gdy:

1. stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
2. stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej, mogą wskazywać na naruszenie zabezpieczeń tych danych.

§3.

1. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nie uprawnionym tożsamości osoby, której dane dotyczą.
2. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.

§4.

1. Każda osoba zatrudniona w Urzędzie Miasta i Gminy w Ostrzeszowie, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób), zobowiązana jest niezwłocznie poinformować o tym osobę zatrudnioną przy przetwarzaniu danych osobowych lub Administratora Bezpieczeństwa Informacji, bądź inną upoważnioną przez niego osobę.
2. Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia danych osobowych, zobowiązana jest niezwłocznie powiadomić o tym Administratora Bezpieczeństwa Informacji.

§5.

Administrator Bezpieczeństwa Informacji, po uzyskaniu informacji o naruszeniu ochrony danych osobowych, powinien w pierwszej kolejności:

1. zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,
2. na bieżąco wygenerować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
3. przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby nieupoważnionej.

§6.

Administrator Bezpieczeństwa Informacji niezwłocznie podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych osobie nieupoważnionej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji, szczególnie poprzez:

1. fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieupoważnionej,
2. wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
3. zmianę haseł oraz czasowe odebranie prawa dostępu użytkownikowi, poprzez którego hasło uzyskano nielegalny dostęp do danych.

§7.

Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba powinna sprawdzić:

1. stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
2. zawartość zbioru danych osobowych,
3. sposób działania programu,
4. wykluczyć możliwość obecności wirusów komputerowych.

§8.

Po dokonaniu powyższych czynności Administrator Bezpieczeństwa Informacji powinien przeprowadzić i przedstawić Administratorowi Danych szczegółową analizę stanu systemu informatycznego obejmującego identyfikację:

1. rodzaju zaistniałego zdarzenia,
2. metody dostępu do danych przez osobę nieupoważnionej,
3. skali zniszczeń.

§9.

Niezwłocznie należy przywrócić normalny stan działania systemy, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, niezbędne jest odtworzenie jej z ostatniej kopii awaryjnej z zachowaniem wszelkich ostrożności, mających na celu uniknięcie ponownego uzyskania dostępu tą samą drogą przez osobę nieupoważnioną.

§10.

Po przywróceniu prawidłowego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

§11.

W tym celu należy zbadać rodzaj przyczyny:

1. jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych w systemie informatycznym, należy przeprowadzić dodatkowe szkolenie wszystkich osób biorących udział przy przetwarzaniu danych,
2. jeżeli przyczyną zdarzenia było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy wyciągnąć konsekwencje,
3. jeżeli przyczyną zdarzenia było uaktywnienie wirusa, należy w miarę możliwości ustalić źródło jego pochodzenia oraz wykonać dodatkowe testy i zabezpieczenia antywirusowe,
4. jeżeli przyczyną zdarzenia był zły stan urządzenia lub sposób działania programu, należy niezwłocznie przeprowadzić kontrolne czynności serwisowo-programowe,
5. jeżeli przyczyną zdarzenia było włamanie w celu pozyskania bazy danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skutecznej ochrony bazy danych.

§12.

Administrator Bezpieczeństwa Informacji przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia (dołączając ewentualne kopie dowodów dokumentujących to zdarzenie) oraz w określonym terminie od daty zaistnienia zdarzenia przekazuje go administratorowi danych.

BURMISTRZ
w.z.
mgr inż. Mariusz Witek
Zastępca Burmistrza